Claims:

1. A method comprising:

responding to a contact point created by a party committing fraud, the response including a set of details, the set of details including a set of false personal information.

- 2. The method of claim 1, comprising responding a plurality of times, each response including a different set of details.
- 3. The method of claim 1, wherein the contact point is an Internet address referring to a web site.
- 4. The method of claim 1, wherein the contact point is an e-mail address.
- 5. The method of claim 1, wherein responding comprises transmitting information at a speed designed to mimic a human entering data.
- 6. The method of claim 1, comprising setting the timing of the responses to resemble that of a set of users responding to a Phishing attack.
- 7. The method of claim 1, wherein each response includes a set of details that are internally consistent.
- 8. The method of claim 1, comprising creating a database including a set of false identities, each false identity including a set of data which is consistent within the set.
- 9. The method of claim 1, wherein each response includes a set of details consistent with an Internet service provider used to respond.
- 10. The method of claim 1, wherein the responding is in response to a Phishing attack.
- 11. The method of claim 1, wherein the responding is conducted using a plurality of Internet access points.
- 12. The method of claim 1, wherein the responding is conducted using a plurality of intermediate networks.
- 13. The method of claim 1, wherein the responding is conducted using a plurality of intermediate Internet service providers.

WO 2005/048522 PCT/US2004/036993

14. The method of claim 1, wherein the data in a response is marked, the method comprising monitoring an institution for the use of marked data in an attempted transaction.

- 15. The method of claim 1, wherein the number of responses is in proportion to a size of an attack in response to which the responses are sent.
- 16. The method of claim 1, wherein responding comprises entering data into a web-form.
- 17. The method of claim 1, comprising marking a response using a cryptographic algorithm, such that the marking is detectable only with a suitable cryptographic key.
- 18. The method of claim 1, wherein the details and the timing of the sending of the data mimic the behavior of automated client software.
- 19. A method comprising:

contacting a plurality of times a website and, with each contact, filling in a web-form with a set data, each set of data including a set of details, the set of details including a set of false personal information.

- 20. The method of claim 19, wherein filling in the web-form comprises transmitting information at a speed designed to mimic a human entering data.
- 21. The method of claim 19, comprising setting the timing of the contacting to resemble that of a set of unrelated users.
- 22. The method of claim 19, wherein each contact includes a set of details that are internally consistent.
- 23. The method of claim 19, comprising creating a database including a set of false identities, each false identity including a set of data which is consistent within the set.
- 24. A system comprising:

a controller to:

respond to a contact point created by a party committing fraud, the response including a set of details, the set of details including a set of false personal information.

WO 2005/048522 PCT/US2004/036993

25. The system of claim 24, wherein the contact point is an Internet address referring to a web site.

- 26. The system of claim 24, wherein the contact point is an e-mail address.
- 27. The system of claim 24, wherein responding comprises transmitting information at a speed designed to mimic a human entering data.
- 28. The system of claim 24, wherein the timing of the responses is to resemble that of a set of users responding to a Phishing attack.
- 29. The system of claim 24, wherein each response includes a set of details that are internally consistent.
- 30. The system of claim 24, comprising a database including a set of false identities, each false identity including a set of data which is consistent within the set.
- 31. The system of claim 24, wherein the responding is conducted using a plurality of intermediate networks.
 - 32. A system comprising:
 - a controller to contact a plurality of times a website and, with each contact, enter a set of data, each set of data including a set of details, the set of details including a set of false personal information.
- 33. The system of claim 32, comprising a database including a set of false identities.
- 34. The system of claim 32, wherein entering the data comprises transmitting information at a speed designed to mimic a human entering data.